SC-PAY GRADE 20

CYBER SECURITY ANALYST

DUTIES AND FEATURES OF THE CLASS:

An incumbent in this class works under the direction of the Director of Information Technology. The work involves safeguarding information system assets by identifying and solving potential and actual security problems as well as the maintenance and administration of security applications within the Information Technology (IT) Department and other departments throughout the County. The work involves assisting with managing various projects with other staff in the IT Department.

EXAMPLES OF WORK:

Protects system by defining access privileges, controls structures and resources; identifying abnormalities and reporting violations; implements security violations and inefficiencies by conducting periodic audits; educates users of potential threats and good business practices; implements and maintains security controls; documents technical support issues; supports the Helpdesk to resolve problems for end users; performs other duties as assigned.

REQUIRED KNOWLEDGE, SKILLS, AND ABILITIES:

Knowledge of Network security maintenance and administration; ability to diagnose related issues; strong knowledge of architecture, engineering and operations of enterprise SIEM platforms; hands-on experience analyzing high volumes of logs, network data and other attached artifacts in support of incident investigations; advanced understanding of TCP/IP , common networking ports and protocols, traffic flow, system administration, OSI model, defense-in-depth and common security elements; experience in vulnerability scanning solutions; understanding of mobile technology, mobile OS and VMware technology; ability to manage projects effectively; must possess strong problem solving and analytical skills in a technical environment including creation and documentation of processes, procedures and problem resolutions; excellent oral and written communication skills; must be self-directed, customer-oriented, quality-oriented, deadline-sensitive, and a team player; must be willing and able to work on multiple tasks within the IT Department; ability to establish and maintain effective working relationships with staff, department heads, elected officials, representatives from other agencies and the general public.

QUALIFICATIONS:

Associate’s degree in Computer Science, Information Systems or equivalent education or work experience; minimum of three (3) + years of prior relevant experience in Cyber Security; advanced certifications such as SANS GIAC/GCIA/GCIH, CISSP or CASP and /or SIEM-specific training and certification a plus; experience with Microsoft Office (Outlook, Word, Excel), SharePoint, Office 365; excellent customer service, organizational, verbal and written communication skills.

ADDITIONAL REQUIREMENTS:

- Direct Deposit Required
- 35-hour work week
- Possession of a valid driver’s license
- Pre-Employment Background Screening
- Pre-Employment Drug/Alcohol Testing
- Must be willing to travel and work nights and weekends occasionally

09/2020